

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-171863

(43)Date of publication of application : 26.06.1998

(51)Int.Cl.

G06F 17/60

(21)Application number : 08-325051

(71)Applicant : HITACHI LTD

(22)Date of filing : 05.12.1996

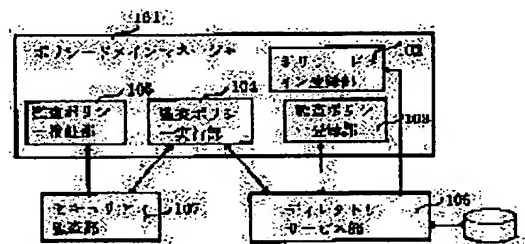
(72)Inventor : NISHIKI KENYA
HIRATA TOSHIAKI
MIYAZAKI SATOSHI

(54) SECURITY AUDIT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a security audit system which is coherent in the entire organization can be obtained, and an audit policy which can be flexibly set according to an organization constitution can be executed.

SOLUTION: This system is provided with a policy domain registering part 102 which registers the execution range of an audit policy indicating the executing method of audit in a directory service part 106, audit policy registering part 103 which registers the audit policy in the directory service part 106, audit policy executing part 104 which sets the registered audit policy in a security audit part 107, and audit policy verifying part 105 which operates the coherence check of the audit policy based on the audit result information of the security audit part 107.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-171863

(43) 公開日 平成10年(1998) 6月26日

(51) Int. Cl. ⁶

G06F 17/60

識別記号

F I

G06F 15/21

Z

審査請求 未請求 請求項の数 4 O L (全 8 頁)

(21) 出願番号 特願平8-325051

(22) 出願日 平成 8 年(1996)12月 5 日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 西木 健哉

神奈川県川崎市麻生区王禅寺1099番地株式
会社日立製作所システム開発研究所内

(72) 発明者 平田 俊明

神奈川県川崎市麻生区王禅寺1099番地株式
会社日立製作所システム開発研究所内

(72) 発明者 宮崎 聡

神奈川県川崎市麻生区王禅寺1099番地株式
会社日立製作所システム開発研究所内

(74) 代理人 弁理士 小川 勝男

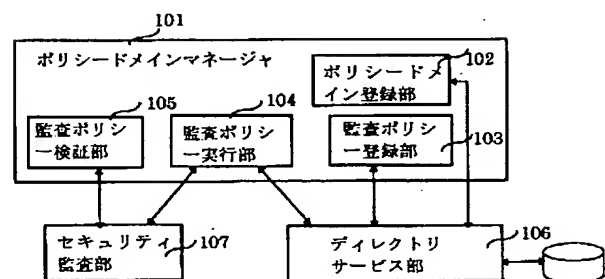
(54) 【発明の名称】 セキュリティ 監査システム

(57) 【要約】

【課題】セキュリティの監査ポリシーをマシン個別あるいは管理するドメイン個別に設定しなければならない手間と、複数の管理者によって管理される場合に監査レベルにばらつきが生じる。

【解決手段】監査の実施方法を表す監査ポリシーの行使範囲をディレクトリサービス部106に登録するポリシードメイン登録部102と、監査ポリシーをディレクトリサービス部106に登録する監査ポリシー登録部103と、登録された監査ポリシーをセキュリティ監査部107に設定する監査ポリシー実行部104と、セキュリティ監査部107の監査結果情報に基づいて監査ポリシーの一貫性チェックを行う監査ポリシー検証部105でなる。

図 1



【特許請求の範囲】

【請求項 1】通信ネットワークによって複数のコンピュータシステムが接続されたインター／イントラネット環境で、ネットワーク資源を論理的な依存関係や包含関係に基づいて階層的に構成しユーザからネットワーク資源へのアクセスを管理するディレクトリサービス部と、ネットワーク資源へのユーザアクセスに関する情報をリアルタイムに収集し記録したり、コンピュータシステム上にインストールされたプログラムの正当性および安全性を確認するセキュリティ監査部とを備えたセキュリティ監査システムにおいて、

監査の実施方法を表す監査ポリシーの行使範囲をディレクトリサービス部に登録するポリシードメイン登録手段と、監査ポリシーをディレクトリサービス部に登録する監査ポリシー登録手段と、登録された監査ポリシーを前記セキュリティ監査部に設定する監査ポリシー実行手段と、セキュリティ監査部の監査結果情報に基づいて監査ポリシーの一貫性チェックを行う監査ポリシー検証手段とを有することを特徴とするセキュリティ監査システム。

【請求項 2】請求項 1 において、前記ポリシードメイン登録手段は、前記監査ポリシー登録手段、監査ポリシー実行手段および監査ポリシー検証手段を実行する主体である監査ポリシーマネージャを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、監査ポリシーマネージャが監査の対象とするオブジェクト名を属性とする被監査オブジェクトを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、前記監査ポリシーマネージャオブジェクトおよび被監査オブジェクトで構成されるポリシードメインを、前記ディレクトリサービス部の上位階層のオブジェクトとして登録する手段とを有するセキュリティ監査システム。

【請求項 3】請求項 1 において、前記監査ポリシー登録手段は、監査対象のオブジェクト種別、監査の有無、監査する項目、監査の行使スケジュール、監査の報告方法に関する属性の入力を受け付けて、前記ディレクトリサービス部の当該監査ポリシーの行使されるポリシードメインオブジェクトの配下のオブジェクトとして登録する手段を有し、前記監査ポリシー実行手段は、前記ディレクトリサービス部の該当する監査ポリシーオブジェクトの属性を取得し、これを監査対象オブジェクトに設定する手段を有するセキュリティ監査システム。

【請求項 4】請求項 1 において、前記監査ポリシー登録手段は、ポリシーオブジェクトがそれが属するポリシードメインの下位のポリシードメインにデフォルトのポリシーオブジェクトとして継承させることの有無を表す属性とポリシー属性の変更を許可することの可否を表す属性の入力を受け付けて、当該オブジェクトに設定する手段を有し、前記ポリシードメイン登録手段は、ポリシードメインをすでに登録されたポリシードメインオブジェ

クトの下位オブジェクトとして登録する手段と、上位のポリシードメインに含まれるポリシーオブジェクトが継承属性を持つ場合に当該ポリシーオブジェクトの複製を作成し、ポリシーの変更属性にあわせてオブジェクトのアクセス権を設定する手段とを有するセキュリティ監査システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はネットワークシステムにおけるセキュリティ監査システムに関するものである。

【0002】

【従来の技術】ネットワーク資源に対する内部あるいは外部からの不正なアクセスに対処するために通常の OS はユーザ認証機構やファイルなどへのアクセス制御機構を備えている。さらにネットワークシステムレベルでのユーザ認証やアクセス制御を実現する技術としてディレクトリサービスと呼ばれる技術が知られており、これによってネットワーク資源を論理的なオブジェクトの階層関係に基づいて一元的に管理することができる。このようなディレクトリサービスについては、“NetWare 4. 1 J ディレクトリサービスの概要”；Novellなどに記載されている。

【0003】またネットワーク資源へのアクセスを逐次ログファイルに登録する監査機構が知られており、このような監査機構については、“Windows NT 3. 5 セキュリティ／監査ガイド”；ASCIIなどに記載されている。

【0004】

【発明が解決しようとする課題】さて、企業などの組織でセキュリティを確保する場合には、セキュリティに関する標準規約を決め組織全体で一貫性のあるものとしなければならない。組織の一部にセキュリティの穴があれば、そこからの不正侵入が組織全体に広がるおそれがある。このような従来技術では、セキュリティの監査ポリシーをマシン個別あるいは管理するドメイン個別に設定しなければならないという手間と、管理者がたとえば部署単位に複数存在する場合には監査レベルにばらつきが生じてしまう問題がある。また監査ポリシーが遵守されているかどうかをチェックする仕掛けも提供されていない。

【0005】本発明の目的は、組織全体で一貫性があり、かつ組織構成に応じて柔軟に設定可能な監査ポリシーを実施することのできるセキュリティ監査システムを提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するために、本発明は、ネットワーク資源を論理的な依存関係や包含関係に基づいて階層的に構成しユーザからネットワーク資源へのアクセスを管理するディレクトリサービス

部と、ネットワーク資源へのユーザアクセスに関する情報をリアルタイムに収集し記録したり、コンピュータシステム上にインストールされたプログラムの正当性および安全性を確認するセキュリティ監査部とを備えたセキュリティ監査システムにおいて、監査の実施方法を表す監査ポリシーの行使範囲をディレクトリサービス部に登録するポリシードメイン登録手段と、監査ポリシーをディレクトリサービス部に登録する監査ポリシー登録手段と、登録された監査ポリシーを前記セキュリティ監査部に設定する監査ポリシー実行手段と、セキュリティ監査部の監査結果情報に基づいて監査ポリシーの一貫性チェックを行う監査ポリシー検証手段とを有するセキュリティ監査システムを提供する。

【0007】また前記ポリシードメイン登録手段は、前記監査ポリシー登録手段、監査ポリシー実行手段および監査ポリシー検証手段を実行する主体である監査ポリシーマネージャを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、監査ポリシーマネージャが監査の対象とするオブジェクト名を属性とする被監査オブジェクトを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、前記監査ポリシーマネージャオブジェクトおよび被監査オブジェクトで構成されるポリシードメインを、前記ディレクトリサービス部の上位階層のオブジェクトとして登録する手段とを有するセキュリティ監査システムを提供する。

【0008】また前記監査ポリシー登録手段は、監査対象のオブジェクト種別、監査の有無、監査する項目、監査の行使スケジュール、監査の報告方法に関する属性の入力を受け付けて、前記ディレクトリサービス部の当該監査ポリシーの行使されるポリシードメインオブジェクトの配下のオブジェクトとして登録する手段を有し、前記監査ポリシー実行手段は、前記ディレクトリサービス部の該当する監査ポリシーオブジェクトの属性を取得し、これを監査対象オブジェクトに設定する手段を有するセキュリティ監査システムを提供する。

【0009】また前記監査ポリシー登録手段は、ポリシーオブジェクトがそれが属するポリシードメインの下位のポリシードメインにデフォルトのポリシーオブジェクトとして継承させることの有無を表す属性とポリシー属性の変更を許可することの可否を表す属性の入力を受け付けて、当該オブジェクトに設定する手段を有し、前記ポリシードメイン登録手段は、ポリシードメインをすでに登録されたポリシードメインオブジェクトの下位オブジェクトとして登録する手段と、上位のポリシードメインに含まれるポリシーオブジェクトが継承属性を持つ場合に当該ポリシーオブジェクトの複製を作成し、さらにポリシーの変更属性にあわせてオブジェクトのアクセス権を設定する手段とを有するセキュリティ監査システムを提供する。

【0010】このようなセキュリティ監査システムによ

れば、監査ポリシーを分散型のデータベース機構を備えるディレクトリサービスを利用して管理しているため、複数の管理者によって分散管理されているシステムにおいても一貫性が保証される。またディレクトリサービスの階層関係を利用して階層化された監査ポリシーを実施でき、柔軟にセキュリティレベルを変更することが可能である。

【0011】

【発明の実施の形態】本発明の第一の実施例を図1に示すセキュリティ監査システムのブロック図を用いて説明する。

【0012】ポリシードメインマネージャ101は、ポリシードメイン単位に監査ポリシーを実行する主体であり、ポリシードメイン登録部102、監査ポリシー登録部103、監査ポリシー実行部104、監査ポリシー検証部105で構成される。ポリシードメイン登録部102、監査ポリシー登録部103、監査ポリシー実行部104はディレクトリサービス部106にアクセスすることができる。また、監査ポリシー実行部104、監査ポリシー検証部105はセキュリティ監査部107にアクセスすることができる。

【0013】また図1に示したセキュリティ監査システムは、たとえば図2に示すような、入力装置204、表示装置205、CPU202、メモリ203、記憶装置206などのハードウェアを備えた電子計算機上に構築することができる。この場合、ポリシードメイン登録部102、監査ポリシー登録部103、監査ポリシー実行部104、監査ポリシー検証部105、ディレクトリサービス部106、セキュリティ監査部107は電子計算機上で実行されるプロセスとして具体化される。

【0014】ディレクトリサービス部106は、たとえばネットワーク・オーエス(NOS)の提供するディレクトリサービスによって実現することができ、ディレクトリ内のオブジェクトは分散データベースのデータとして管理される。またセキュリティ監査部107は監査対象である各電子計算機のオーエス(OS)が提供する監査インターフェースを使用して実現することができる。

【0015】図3のネットワークシステム構成図を用いて、監査ポリシーを実施する全体フローを説明する。図3ではポリシードメインとしてセンタードメイン301と営業店ドメイン302が存在する。まずセンタードメイン301においてポリシードメインマネージャであるPDM303のポリシードメイン登録処理部で前記2つのポリシードメインをディレクトリサービス部であるDS304に登録する。このとき営業店ドメインオブジェクトはセンタードメインオブジェクトの下位に位置するオブジェクトとして登録する。

【0016】次にPDM-1の監査ポリシー登録部がたとえばサーバの監査を行うための監査ポリシーをディレクトリサービス部DS-1に登録する。PDM303の

監査ポリシー実行部はDS-1に登録されている監査ポリシーをセンタードメイン内のサーバオブジェクトであるサーバ305、サーバ306などに対して設定する。さらにDS304に登録されたポリシードメインオブジェクトおよび監査ポリシーオブジェクトはディレクトリサービスの提供するディレクトリ同期処理によって営業店ドメイン内のディレクトリサービス部DS307の参照するデータベースに反映される。営業店ドメインのポリシードメインマネージャであるPDM308の監査ポリシー実行部はセンタードメインで設定されたサーバに

10 関する監査ポリシーを継承し、営業店ドメイン内のサーバオブジェクトであるサーバ309、サーバ310などに対して設定する。またPDM308の監査ポリシー登録部はPDM303で登録された監査ポリシーとは別の監査ポリシーを登録し、実行することも可能である。

【0017】またPDM303の監査ポリシー検証部は、監査ポリシーの登録および実行処理とは独立に管理者の指示したタイミングで実行される。

【0018】次に図4のフローチャートを用いてポリシードメイン登録処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサービス部に接続する(401)。既存ドメインが登録されている場合には新規ドメインと既存ドメインとの間に継承関係を設定するかどうかを選択させ(402)、継承関係を設定する場合には既存ドメインの上位あるいは下位にドメインオブジェクトを登録する(403)。オブジェクトはディレクトリサービス部によって管理可能なたとえば図8~図10の形式で格納する。

【0019】図8に示すディレクトリオブジェクト構成テーブル800は、対応するオブジェクトを識別するためのオブジェクト識別子801、オブジェクトの階層構造上の位置を示すオブジェクト位置識別子802、ネットワーク資源の種別を示すオブジェクトタイプ803、アクセス権利テーブルへのポインタ804、オブジェクトプロパティテーブルへのポインタ805、および次のテーブルエントリへのポインタ806からなる。図9に示すアクセス権利テーブル900は、オブジェクトへのアクセス権利を保有するオブジェクト識別名901、オブジェクトアクセスもしくはプロパティアクセスを示すアクセスタイプ902、およびオブジェクトに記憶された情報の参照、更新などの内容を示すアクセス権利903からなる。図10に示すオブジェクトプロパティテーブル1000は、プロパティ1001、プロパティ値1002、および次のテーブルエントリへのポインタ1003からなる。

【0020】次に図5のフローチャートを用いて監査ポリシー登録処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサービス部に接続し(501)、登録されたポリシードメインのなかから監査ポリシーを作成するポリシードメインを選択する。こ

の場合、ポリシードメインマネージャは選択したポリシードメインオブジェクトに対する適切なアクセス権を保有している必要がある。次に監査対象のオブジェクト種別、監査の有無、監査する項目(たとえばログオン/ログオフ、ファイルアクセス、ユーザとグループの設定、システム再起動などについての成功あるいは失敗)、監査の行使スケジュール、監査の報告方法(たとえばログファイルに登録する、指定されたユーザにメッセージを送信など)をそれぞれプロパティとして持つ監査ポリシーオブジェクトとして、ドメインオブジェクトの配下に登録する(503)。既存の監査ポリシーを選択して特定のプロパティを変更することも可能である。次に登録された監査ポリシーを下位のポリシードメインに継承させるかどうかを選択し(504)、継承させる場合には継承属性をオブジェクトに付加する(505)。さらに継承された監査ポリシーの変更を許可するかどうかを選択し(506)、変更を許可する場合には変更可能属性をオブジェクトに付加する(507)。

【0021】次に図6のフローチャートを用いて監査ポリシー実行処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサーバに接続し(601)、ポリシードメインマネージャの管理する監査対象オブジェクトの情報および監査ポリシー情報を取得する(602)。監査ポリシーのオブジェクト種別にあてはまる監査対象オブジェクトについてオブジェクトを管理するセキュリティ監査部にアクセスして、監査ポリシーの内容を設定する(603)。

【0022】次に図7のフローチャートを用いて監査ポリシー検証処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサーバに接続し(701)、監査ポリシー情報を取得し、現在監査対象となっているオブジェクトを特定する(702)。次にオブジェクトを管理するセキュリティ監査部にアクセスし、監査結果情報(たとえばセキュリティログファイル)を取得し(703)、監査ポリシーに従って監査が行われているかどうかをチェックする(704)。チェックは管理者の判断で行うケースとチェックプログラムを使用して行うケースにわかれる。またポリシードメインの配下にポリシードメインが存在する場合には(705)、配下ポリシードメインマネージャを起動して監査ポリシーの検証を行う(706)。配下のドメインに監査ポリシーを継承させており、かつ監査ポリシーの変更を許可していない場合には上位の監査ポリシーに照らして検証を行う。監査ポリシー違反が検出された場合にはポリシードメインの管理者に特定のアラームをあげることによってこれを通知する。

【0023】本実施例のセキュリティ監査システムによれば、監査ポリシーを分散型のデータベース機構を備えるディレクトリサービスを利用して管理しているので、複数の管理者によって分散管理されているシステムにお

いても一貫性が保証される。ディレクトリサービスの階層関係を利用して階層化された監査ポリシーを実施でき、柔軟にセキュリティレベルを変更することが可能である。

【0024】

【発明の効果】本発明では、ポリシードメイン登録手段によってセキュリティレベルに対応した階層的な管理ドメインを構築でき、監査ポリシー登録、実行、検証手段によって監査ポリシーを分散型のデータベース機構を備えるディレクトリサービスを利用して管理しているの

10

【図面の簡単な説明】

【図1】本発明の実施例のシステムのブロック図。

【図2】本発明の実施例のシステムのハードウェアのブロック図。

【図3】本発明の実施例のセキュリティ監査システムのブロック図。

【図1】

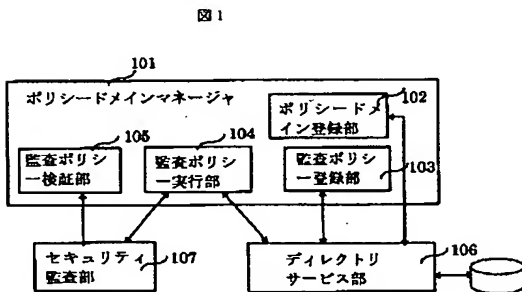


図1

【図4】本発明の実施例のポリシードメインの登録のフローチャート。

【図5】本発明の実施例の監査ポリシーの登録のフローチャート。

【図6】本発明の実施例の監査ポリシーの実行のフローチャート。

【図7】本発明の実施例の監査ポリシーの検証のフローチャート。

【図8】本発明の実施例のディレクトリオブジェクトテーブルの形式を示す説明図。

【図9】本発明の実施例のアクセス権利エントリの形式を示す説明図。

【図10】本発明の実施例のオブジェクトプロパティテーブルの形式を示す説明図。

【符号の説明】

101…ポリシードメインマネージャ、

102…ポリシードメイン登録部、

103…監査ポリシー登録部、

104…監査ポリシー実行部、

20 105…監査ポリシー検証部、

106…ディレクトリサービス部、

107…セキュリティ監査部。

【図2】

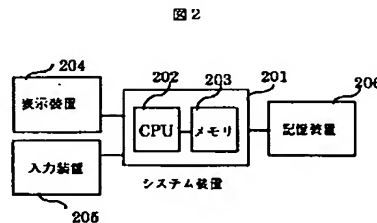


図2

【図8】

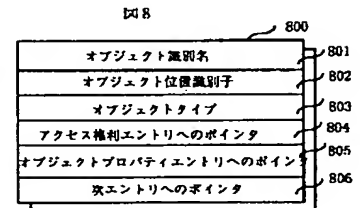


図8

【図3】

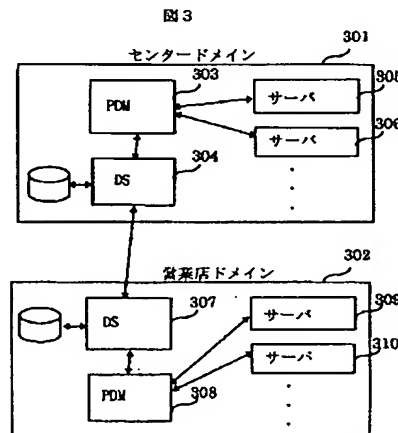


図3

【図9】

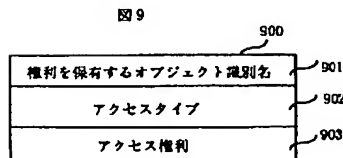
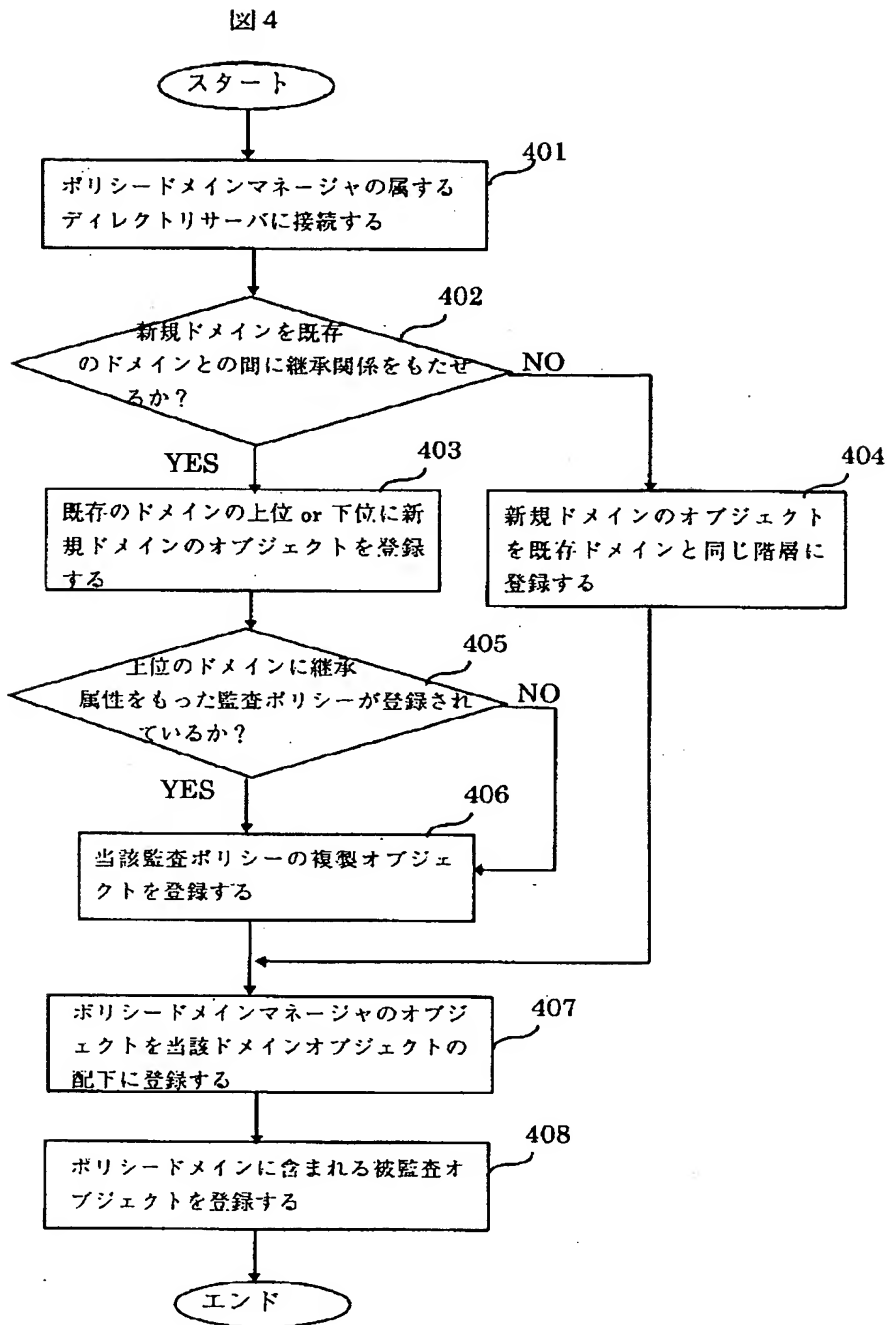
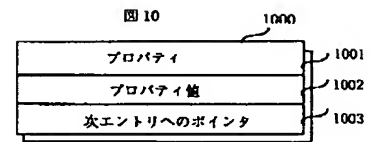


図9

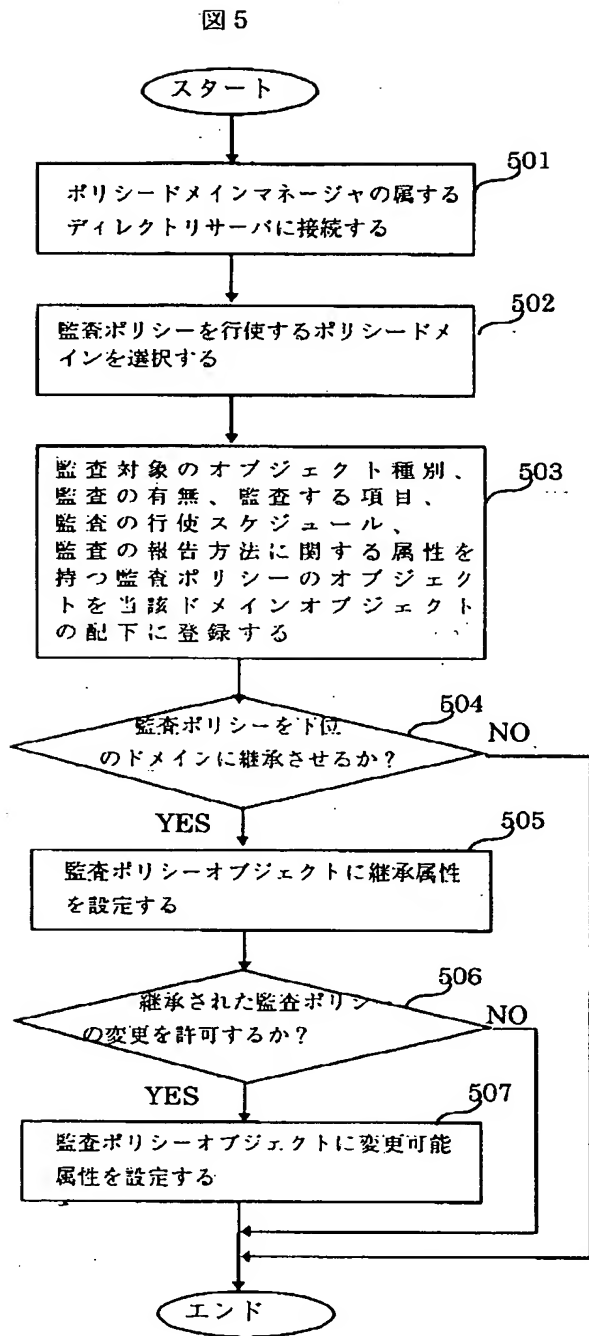
【図 4】



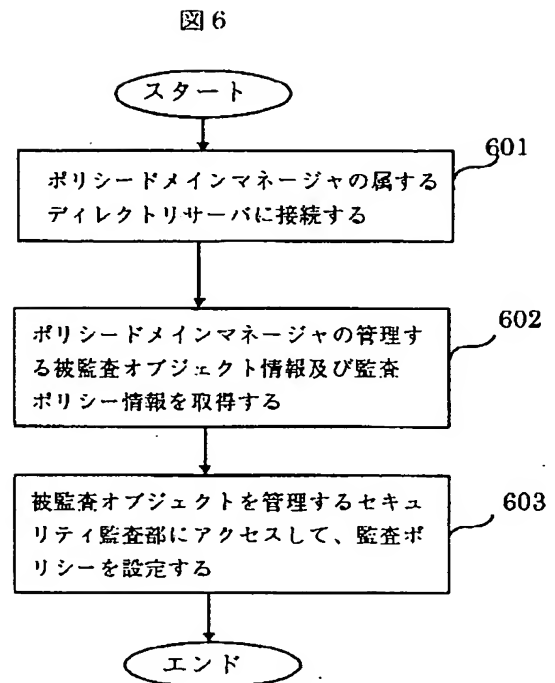
【図 10】



【図 5】



【図 6】



【図 7】

図 7

